

DRAFT INTERNATIONAL STANDARD

ISO/SAE DIS 21434

ISO/TC 22/SC 32

Secretariat: JISC

Voting begins on:
2020-02-12

Voting terminates on:
2020-05-06

Road vehicles — Cybersecurity engineering

ICS: 43.040.15

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/SAE DIS 21434](#)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.



Reference number
ISO/SAE DIS 21434:2020(E)

© ISO/SAE International 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/SAE DIS 21434

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>



COPYRIGHT PROTECTED DOCUMENT

© ISO/SAE International 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced, or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or SAE International at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
400 Commonwealth Dr.
Warrendale, PA, USA 15096
Phone: 877-606-7323 (inside USA and Canada)
Phone: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
Website: www.sae.org

Published in Switzerland by ISO, published in the USA by SAE International

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/SAE DIS 21434

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

CONTENTS

1.	SCOPE.....	10
2.	NORMATIVE REFERENCES	10
3.	TERMS AND ABBREVIATIONS	10
3.1	Terms and Definitions	10
3.2	Abbreviated Terms.....	14
4.	GENERAL CONSIDERATIONS	14
5.	OVERALL CYBERSECURITY MANAGEMENT	16
5.1	General.....	16
5.2	Objectives	16
5.3	Inputs.....	17
5.3.1	Prerequisites	17
5.3.2	Further Supporting Information	17
5.4	Requirements and Recommendations.....	17
5.4.1	Cybersecurity Governance	17
5.4.2	Cybersecurity Culture.....	18
5.4.3	Cybersecurity Risk Management	19
5.4.4	Organizational Cybersecurity Audit.....	19
5.4.5	Information Sharing.....	20
5.4.6	Management Systems	20
5.4.7	Tool Management	21
5.4.8	Information Security Management.....	21
5.5	Work Products.....	21
6.	PROJECT DEPENDENT CYBERSECURITY MANAGEMENT	22
6.1	General.....	22
6.2	Objectives	22
6.3	Inputs.....	23
6.3.1	Prerequisites.....	23
6.3.2	Further Supporting Information.....	23
6.4	Requirements and Recommendations.....	23
6.4.1	Cybersecurity Responsibilities and Their Assignment.....	23
6.4.2	Cybersecurity Planning	23
6.4.3	Tailoring of the Cybersecurity Activities	24
6.4.4	Reuse	25
6.4.5	Component Out of Context	26
6.4.6	Off-the-Shelf Component	26
6.4.7	Cybersecurity Case	26
6.4.8	Cybersecurity Assessment.....	26
6.4.9	Release for Post-Development	28
6.5	Work Products.....	29
7.	CONTINUOUS CYBERSECURITY ACTIVITIES	29
7.1	General.....	29
7.2	Objectives	29
7.3	Cybersecurity Monitoring	29
7.3.1	Inputs.....	29
7.3.2	Requirements and Recommendations.....	30
7.3.3	Work Products.....	30
7.4	Cybersecurity Event Assessment	30
7.4.1	Inputs.....	30
7.4.2	Requirements and Recommendations.....	31
7.4.3	Work Products.....	31

7.5	Vulnerability Analysis	31
7.5.1	Inputs.....	31
7.5.2	Requirements and Recommendations.....	31
7.5.3	Work Products.....	32
7.6	Vulnerability Management	32
7.6.1	Inputs.....	32
7.6.2	Requirements and Recommendations.....	32
7.6.3	Work Products.....	33
8.	RISK ASSESSMENT METHODS	33
8.1	General.....	33
8.2	Objectives	34
8.3	Asset Identification	34
8.3.1	Inputs.....	34
8.3.2	Requirements and Recommendations.....	34
8.3.3	Work Products.....	35
8.4	Threat Scenario Identification	35
8.4.1	Inputs.....	35
8.4.2	Requirements and Recommendations.....	35
8.4.3	Work Products.....	36
8.5	Impact Rating	36
8.5.1	Inputs.....	36
8.5.2	Requirements and Recommendations.....	36
8.5.3	Work Products.....	37
8.6	Attack Path Analysis	37
8.6.1	Inputs.....	37
8.6.2	Requirements and Recommendations.....	37
8.6.3	Work Products.....	38
8.7	Attack Feasibility Rating	39
8.7.1	Inputs.....	39
8.7.2	Requirements and Recommendations.....	39
8.7.3	Work Products.....	40
8.8	Risk Determination.....	40
8.8.1	Inputs.....	40
8.8.2	Requirements and Recommendations.....	40
8.8.3	Work Products.....	40
8.9	Risk Treatment Decision	40
8.9.1	Inputs.....	40
8.9.2	Requirements and Recommendations.....	41
8.9.3	Work Products.....	41
9.	CONCEPT PHASE	41
9.1	General.....	41
9.2	Objectives	42
9.3	Item Definition	42
9.3.1	Inputs.....	42
9.3.2	Requirements and Recommendations.....	42
9.3.3	Work Products.....	43
9.4	Cybersecurity Goals.....	43
9.4.1	Inputs.....	43
9.4.2	Requirements and Recommendations.....	44
9.4.3	Work Products.....	45
9.5	Cybersecurity Concept.....	45
9.5.1	Inputs.....	45
9.5.2	Requirements and Recommendations.....	46
9.5.3	Work Products.....	46
10.	PRODUCT DEVELOPMENT	46
10.1	General.....	46
10.2	Objectives	49
10.3	Inputs.....	49
10.3.1	Prerequisites	49
10.3.2	Further Supporting Information	50

10.4	Requirements and Recommendations.....	50
10.4.1	Refinement of Cybersecurity Requirements and Architectural Design.....	50
10.4.2	Integration and Verification	53
10.4.3	Specific Requirements for Software Development	56
10.5	Work Products.....	57
11.	CYBERSECURITY VALIDATION	57
11.1	General.....	57
11.2	Objectives	57
11.3	Inputs.....	57
11.3.1	Prerequisites	57
11.3.2	Further Supporting Information	58
11.4	Requirements and Recommendations.....	58
11.5	Work Products.....	58
12.	PRODUCTION	58
12.1	General.....	58
12.2	Objectives	58
12.3	Inputs.....	59
12.3.1	Prerequisites	59
12.3.2	Further Supporting Information	59
12.4	Requirements and Recommendations.....	59
12.5	Work Products.....	60
13.	OPERATIONS AND MAINTENANCE.....	60
13.1	General.....	60
13.2	Objectives	60
13.3	Cybersecurity Incident Response	60
13.3.1	Inputs.....	60
13.3.2	Requirements and Recommendations.....	60
13.3.3	Work Products.....	61
13.4	Updates.....	61
13.4.1	Inputs.....	61
13.4.2	Requirements and Recommendations.....	62
13.4.3	Work Products.....	62
14.	DECOMMISSIONING	62
14.1	General.....	62
14.2	Objectives	62
14.3	Inputs.....	62
14.3.1	Prerequisites	62
14.3.2	Further Supporting Information	62
14.4	Requirements and Recommendations.....	63
14.5	Work Products.....	63
15.	DISTRIBUTED CYBERSECURITY ACTIVITIES.....	63
15.1	General.....	63
15.2	Objectives	63
15.3	Inputs.....	63
15.3.1	Prerequisites	63
15.3.2	Further Supporting Information	63
15.4	Requirements and Recommendations.....	63
15.4.1	Demonstration and Evaluation of Supplier Capability.....	63
15.4.2	Request for Quotation	64
15.4.3	Alignment of Responsibilities	64
15.5	Work Products.....	65

ITC STANDARD PREVIEW

(standards.iteh.ai)

ISO/SAE DIS 21434

[https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

[df3296059a5e/iso-sae-dis-21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

ANNEX A (INFORMATIVE)	SUMMARY OF CYBERSECURITY ACTIVITIES AND WORK PRODUCTS	66
ANNEX B (INFORMATIVE)	EXAMPLES OF CYBERSECURITY CULTURE	68
ANNEX C (INFORMATIVE)	CYBERSECURITY INTERFACE AGREEMENT TEMPLATE EXAMPLE	69
ANNEX D (INFORMATIVE)	CYBERSECURITY RELEVANCE: EXAMPLE METHOD AND CRITERIA	71
ANNEX E (INFORMATIVE)	CYBERSECURITY ASSURANCE LEVELS	72
ANNEX F (INFORMATIVE)	VERIFICATION AND VALIDATION	77
ANNEX G (INFORMATIVE)	EXAMPLE USE CASE AND WORK PRODUCTS: HEADLAMP SYSTEM	80
ANNEX H (INFORMATIVE)	IMPACT RATING FOR SAFETY, FINANCIAL, OPERATIONAL AND PRIVACY DAMAGE	97
ANNEX I (INFORMATIVE)	GUIDELINES FOR DETERMINING ATTACK FEASIBILITY RATING	99
ANNEX J (INFORMATIVE)	MATRICES FOR RISK DETERMINATION	105

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/SAE DIS 21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

FOREWORD

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

SAE Technical Standards Board Rules provide that: "This document is published to advance the state of technical and engineering sciences. The use of this document is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was jointly prepared by Technical Committee ISO/TC 22, Road vehicles, Subcommittee SC 32, Electrical and electronic components and general system aspects, and SAE Vehicle Cybersecurity Systems Engineering Committee.

This first edition of ISO/SAE 21434 cancels and supersedes SAE J3061_201601.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html. Alternatively, to provide feedback on this document, please visit <http://standards.sae.org/PRODCODE>.

INTRODUCTION

Purpose of this Document

This document addresses the cybersecurity perspective in engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with changing technology and attack methods.

This document provides vocabulary, objectives, requirements and guidelines as a foundation for common understanding throughout the supply chain. This enables organizations to:

- define cybersecurity policies and processes;
- manage cybersecurity risk; and
- foster a cybersecurity culture.

This document can be used to implement a cybersecurity management system including cybersecurity risk management in accordance with ISO 31000. This document is intended to supersede SAE J3061 recommended practice.

Organization of this Document

An overview of the document structure is given in Figure 1. The elements of Figure 1 do not prescribe an execution sequence of the individual topics.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/SAE DIS 21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

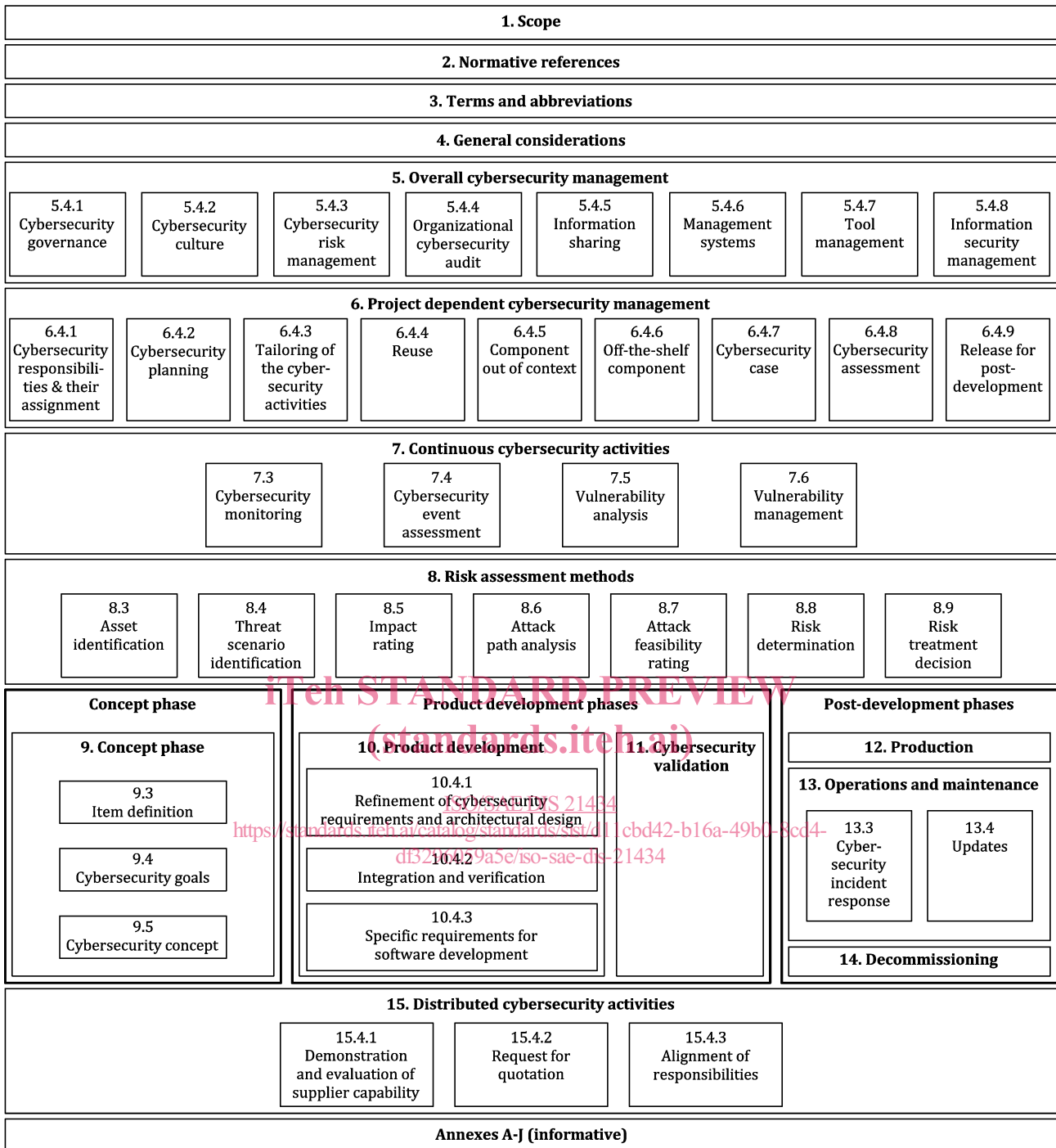


Figure 1 - Overview of this document

Clauses 5 and 6 (Management of Cybersecurity) include the implementation of the organizational cybersecurity policy, rules, and processes for overall cybersecurity management and for project dependent cybersecurity management.

Clause 7 (Continuous Cybersecurity Activities) defines activities that provide information for ongoing risk assessments and vulnerability management of E/E systems until end of support.

Clause 8 (Risk Assessment Methods) defines methods to determine the extent of cybersecurity risk.

Clause 9 (Concept Phase) defines an item and the relevant assets, provides cybersecurity risk determination, and defines the cybersecurity goals.

Clause 10 (Product Development) defines the cybersecurity specification, implements and verifies cybersecurity requirements specific to an item or component.

Clause 11 (Cybersecurity Validation) describes the cybersecurity validation of an item at the vehicle level.

Clause 12 (Production) specifies the cybersecurity related aspects of fabrication, assembly and/or calibration of an item or component.

Clause 13 (Operations and Maintenance) specifies activities related to cybersecurity incident response and updates to an item or component.

Clause 14 (Decommissioning) includes cybersecurity considerations that relate to the decommissioning of an item or component.

Clause 15 (Distributed Activities) includes requirements for supplier management.

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/SAE DIS 21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

1. SCOPE

This document specifies requirements for cybersecurity risk management regarding engineering for concept, development, production, operation, maintenance, and decommissioning for road vehicle electrical and electronic (E/E) systems, including their components and interfaces.

A framework is defined that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk.

This document is applicable to series production road vehicle E/E systems, including their components and interfaces whose development or modification began after the publication of the document.

This document does not prescribe specific technology or solutions related to cybersecurity.

2. NORMATIVE REFERENCES

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 31000, Risk management - Guidelines

ISO 26262-3:2018, Road vehicles - Functional Safety - Part 3: Concept phase

3. TERMS AND ABBREVIATIONS

3.1 Terms and Definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4->

ISO Online browsing platform: available at <http://www.iso.org/obp>

IEC Electropedia: available at <http://www.electropedia.org/>

3.1.1 ASSET

Something for which the compromise of its *cybersecurity properties* (3.1.17) can lead to damage to an *item's* (3.1.21) *stakeholder* (3.1.29).

3.1.2 ATTACK

Attempted deliberate action or interaction with the item or component or its environment that has the potential to result in an adverse consequence.

3.1.3 ATTACK FEASIBILITY

Qualified attribute of an *attack path* (3.1.4) describing the ease of successfully carrying out the corresponding *attack* (3.1.2).

3.1.4 ATTACK PATH

Set of actions that could lead to the realization of a *threat scenario* (3.1.31).

3.1.5 ATTACKER

Person, group, or organization that conducts an *attack* (3.1.2).

36 3.1.6 AUDIT

37 Examination of an implemented process to determine the extent to which the process objectives are fulfilled.

38 [Modified from SOURCE: ISO 26262-1:2018^[1]]

39 3.1.7 CUSTOMER

40 Person or organization that receives a service or product.

41 [Modified from SOURCE: ISO 9000]

42 3.1.8 CYBERSECURITY

43 Road Vehicle Cybersecurity

44 Condition in which *assets* (3.1.1) are sufficiently protected against threat scenarios to electrical or electronic components
45 of road vehicles and their functions.

46 Note 1 to Entry: In this document, for the sake of brevity, only the term cybersecurity is used.

47 3.1.9 CYBERSECURITY ASSESSMENT

48 Judgement of the achieved degree of *cybersecurity* (3.1.8).

49 3.1.10 CYBERSECURITY CLAIM

50 Statement on a *risk* (3.1.25) that is accepted.

51 Note to Entry: Includes a description of why the risk is acceptable and a specification under which conditions the risk
52 needs to be re-evaluated.

53 3.1.11 CYBERSECURITY CONCEPT

54 Collection of allocated cybersecurity requirements which achieve identified *cybersecurity goals* (3.1.14).

55 3.1.12 CYBERSECURITY CONTROL

56 Measure that is modifying *risk* (3.1.25).

57 [Modified from SOURCE: ISO 31000:2018]

58 3.1.13 CYBERSECURITY EVENT

59 *Cybersecurity information* (3.1.15) that has been confirmed as potentially relevant to an *item* (3.1.21) or component.

60 3.1.14 CYBERSECURITY GOAL

61 Concept level cybersecurity requirement associated with one or more *threat scenarios* (3.1.31).

62 Note to Entry: The statement of the cybersecurity goal can refer to an asset, attack path or to the damage scenario
63 associated with the threat scenario.

64 3.1.15 CYBERSECURITY INFORMATION

65 Information derived from data collected by the monitoring process for which relevance to an item or component has not
66 been determined.

68 3.1.16 CYBERSECURITY INTERFACE AGREEMENT

69 Agreement between *customer* (3.1.7) and supplier concerning distributed cybersecurity activities.

70 3.1.17 CYBERSECURITY PROPERTY

71 Attribute of an *asset* (3.1.1) including confidentiality, integrity, and availability.

72 3.1.18 DAMAGE SCENARIO

73 Adverse consequence or undesirable result due to the compromise of a *cybersecurity property* (3.1.16) (or properties)
74 of an *asset* (3.1.1), or of a group of *assets*.

75 3.1.19 EMBEDDED SOFTWARE

76 Fully-integrated software to be executed on a processing element.

77 [SOURCE: ISO 26262-1:2018^[1]]

78 3.1.20 IMPACT

79 Estimate of magnitude of damage or physical harm from a *damage scenario* (3.1.18).

80 3.1.21 ITEM

81 System or combination of systems to implement a function at the vehicle level.

82 [Modified from SOURCE: ISO 26262-1:2018^[1]]

83 3.1.22 OUT OF CONTEXT

84 Not developed in the context of a specific *item* (3.1.21). [SAE DIS 21434](https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434)

<https://standards.iteh.ai/catalog/standards/sist/d11cbd42-b16a-49b0-8cd4-df3296059a5e/iso-sae-dis-21434>

85 3.1.23 PENETRATION TESTING

86 Cybersecurity testing in which real-world attacks are mimicked to identify ways to compromise *cybersecurity goals*
87 (3.1.14).

88 [SOURCE: NIST SP 800-115^[21]]

89 3.1.24 RESIDUAL RISK

90 *Risk* (3.1.25) remaining after risk treatment.

91 [SOURCE: ISO/IEC 27000^[9]]

92 3.1.25 RISK

93 Effect of uncertainty on *road vehicle cybersecurity* (3.1.8) expressed in terms of *attack feasibility* (3.1.3) and *impact*
94 (3.1.20).

95 [Modified from SOURCE: ISO 31000:2018]

96 3.1.26 RISK MANAGEMENT

97 Coordinated activities to direct and control an organization with regard to *risk* (3.1.25).

98 [Modified from SOURCE: ISO 31000:2018]

99

100 3.1.27 ROAD USER

101 Person who uses a road, such as a pedestrian, cyclist, motorist, or an actor providing transportation.

102 3.1.28 SERIES PRODUCTION ROAD VEHICLE

103 Road vehicle that is intended primarily to be used for public roads and is not a prototype.

104 Note 1 to Entry: Vehicle type classification can vary between regions.

105 EXAMPLE 1: A vehicle that is sold for use by the general public.

106 EXAMPLE 2: A vehicle that is sold to be used amongst the general public.

107 [Modified from SOURCE: ISO 26262-1:2018^[1]]

108 3.1.29 STAKEHOLDER

109 Person or organization that can be affected by a *damage scenario* (3.1.18).

110 [Modified from SOURCE: ISO 31000:2018]

111 3.1.30 TARGET ENVIRONMENT

112 Environment on which specific software is intended to be executed.

113 EXAMPLE 1: For application software the target environment is the microcontroller and its software.

114 EXAMPLE 2: For embedded software the target environment is the ECU in the system context.

115 3.1.31 THREAT SCENARIO

116 Statement of potential negative actions that lead to a *damage scenario* (3.1.18).

117 3.1.32 TRIAGE

118 Analysis to determine the relevance of *cybersecurity information* (3.1.15) to an item or component.

119 3.1.33 TRIGGER

120 Criterion used by cybersecurity monitoring for *triage* (3.1.32).

121 3.1.34 VALIDATION

122 Confirmation, through the provision of objective evidence, that the cybersecurity goals of the item are adequate and are
123 achieved.

124 [Modified from SOURCE: ISO/IEC/IEEE 15288:2015^[14]]

125 3.1.35 VERIFICATION

126 Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

127 [SOURCE: ISO/IEC/IEEE 15288:2015^[14]]

128